(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
25 October 2001 (25.10.2001)

PCT

(10) International Publication Number
WO 01/80525 A1

(51) International Patent Classification[7]: H04L 29/06

(21) International Application Number: PCT/US01/05261

(22) International Filing Date: 16 February 2001 (16.02.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/549,622 14 April 2000 (14.04.2000) US

(71) Applicant: SUN MICROSYSTEMS, INC. [US/US]; 901 San Antonio Road, Palo Alto, CA 94303 (US).

(72) Inventor: HANS, Sebastian, Juergen; Werdstrasse 129, CH-8003 Zuerich (CH).

(74) Agent: KIVLIN, B., Noel; Conley, Rose & Tayon, P.C., P.O. Box 398, Austin, TX 78767-0398 (US).

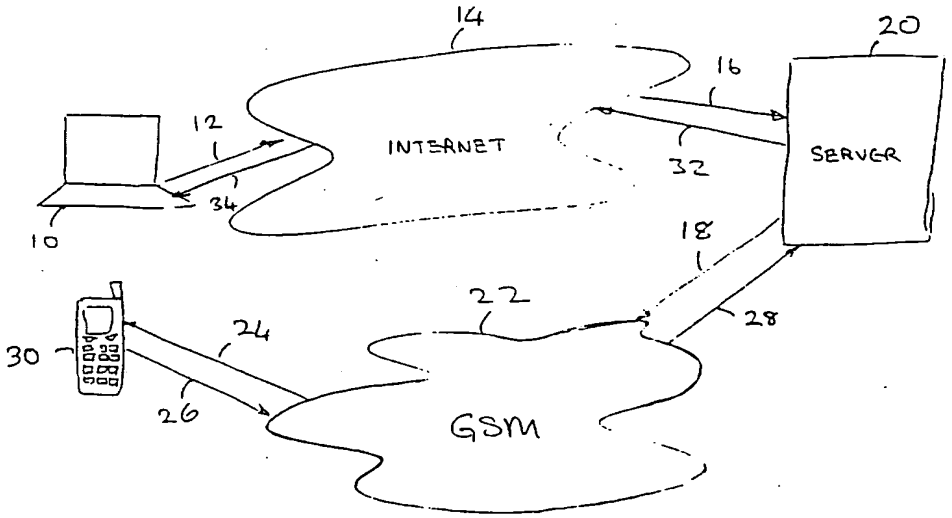
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: NETWORK ACCESS SECURITY



(57) Abstract: A network security system controls access to a resource. A client station provides for inputting an access request for access to a resource via a network, for example the Internet. The access request identifies the user and the resource to be accessed. A server holds data regarding users including a contact address for a communications device of the user and is responsive to the access request to issue an authentication request to the communications device. A communications device includes a receiver for receiving the authentication request from the network resource, a controller operable to invite a user to input a response to the authentication request and a transmitter to return the response to the server. The server is further operable to evaluate a received response for determining whether the user is permitted to gain access to the resource. Authentication of requests for access to resources via a network is provided in a flexible manner using readily available components in a flexible manner, for example a mobile telephone.

WO 01/80525 A1

TITLE: NETWORK ACCESS SECURITY

BACKGROUND OF THE INVENTION

The invention relates to the control of access to a resource via a network.

Identifying a user over a network, for example over a public network such as the Internet, can be a problem where a user wishes to gain access to a resource such as a closed user group and/or to a virtual private network via the public network. It has been proposed to address this problem in a number of ways.

Typically, this problem has been solved by providing a security token in the form of a smart card, or some other piece of special purpose hardware for encrypting and decrypting data. The user has possession of the token and additionally some further information that only the user knows, for example a Personal Identification Number (PIN). The token and the PIN can then be used to identify the user in some secure way using a secure protocol between a client station at which the user is located and a server.

However, such a solution requires the client station to have suitable equipment for interfacing with the token. For example, a smart card reader must be provided for interfacing with a smart card, where this is used as the token. Although the token may be portable, if it is a special smart card or some other form of special purpose hardware, the need for a reader means that this form of solution to the problem is not as flexible as might at first seem to be the case.

Accordingly, an aim of the present invention is to provide an improved method, apparatus and system of providing secure access to resources via a network.

SUMMARY OF THE INVENTION

Particular and preferred aspects of the invention are set out in the accompanying independent and dependent claims. Combinations of features from the dependent claims may be combined with features of the independent claims as appropriate and not merely as explicitly set out in the claims.

In accordance with one aspect of the invention, there is provided a network access security system. A client station provides for inputting an access request for access to a resource via a network, for example the Internet, the access request identifying the user. A server holds data regarding users including a contact address for a communications device of the user and is responsive to the access request to issue an authentication request to the communications device. A communications device includes a receiver for receiving the authentication request from the server, a controller operable to invite a user to input a response to the authentication request and a transmitter to return the response to the server. The server is further operable to evaluate a received response for determining whether the user is permitted to gain access to the resource.

An embodiment of the invention enables authentication of requests for access to resources via a network using readily available components in a flexible manner. Thus, authentication can be achieved without the use of specific hardware of the types required by prior art approaches described above. Where the communications device is a mobile (cellular) telephone or the like, the actual device used to provide authentication is portable and can be carried by the user. The user can request access to the required resource from any available computer or web

access device without needed to carry equipment that he or she would not otherwise carry with him- or herself anyway.

Thus, in an advantageous embodiment, at least one of the receiver and the transmitter includes a wireless communications interface, whereby the communications device is capable of wireless communication. For example the communications device can be a mobile telephone.

Where, for example the communications device is a GSM (Global System for Mobiles) compatible device, the ownership of the device can be achieved by means of a user identification unit such as a Subscriber Identity Module (SIM) card. A SIM card holds a unique identification that is registered with a network service provider as belonging to a specific user.

In an embodiment of the invention the authentication request messages and/or the response message can be in the form of a text message, for example in accordance with the Short Message Service messaging protocol.

In accordance with another aspect, the invention provides a communications device including a receiver for receiving a resource access authentication request from a server, a controller operable to invite a user to input a response to the authentication request and a transmitter to return the response to the server for gaining access to the resource.

In accordance with a further aspect, the invention provides a server including a network message interface for receiving an access request from a client station for access to a resource, the access request identifying the user, a server holding data relating to users including a contact address for a communications device for users, the server being responsive to a received access request to issue an authentication request to the communications device of a user identified in the access request.

The server can include a directory holding data relating to users including at least a contact address for a communications device for the user, and a controller responsive to receipt of an access request to retrieve a contact address from the directory for the user and to issue an authentication request to the communications device.

In an embodiment of the invention, the authentication request is directed via a message service for calling the communications device of the user. Alternatively, this function can be integral to the server.

The directory can hold required responses to authentication requests, the controller being operable to compare a response from the communications device to a required response to determine whether to permit access to the resource.

In accordance with yet a further aspect of the invention, the invention provides user input equipment for input of a resource access request and a network interface for issuing an access request to a server for access to a network, where the access request identifies the user and the resource to be accessed.

In accordance with a yet another aspect of the invention, there is provided a method of controlling access to a network resource. The method includes a number of steps. In response to input of an access request by a user for access to a resource at a network client, an access request is sent to a server, the access request identifying the user. At the server, receipt of the access request causes a unique contact address for a communications device for the user identified in the access request to be retrieved and an authentication request to be issued to the communications device. At the communications device, on receipt of the authentication request, a user is invited to input a response to the authentication request. On input of a response by the user, the response is sent to the server.

At the server, the response is evaluated and, in the event a valid response is received, access to the resource is allowed.

In accordance with a further aspect of the invention, there is provided a computer program, the computer program comprising program instructions for controlling a server: to retrieve, from a directory, a contact address for a communications device of a user associated with a user identification in a resource access request received from a client station; to issue an authentication request to the communications device at the retrieved address; and to evaluate a response received from the communications device and to permit access to the requested resource only where a valid response is received. The computer program product can be provided on a carrier medium, for example a storage medium or a transmission medium.

In accordance with a further aspect of the invention, there is provided a computer program for controlling a proactive validation unit in mobile equipment, the computer program comprising program instructions to validate an authentication message received from a server, to prompt a user to input a response, to prepare an authentication response message and to forward an authentication response message to the server.

DESCRIPTION OF PARTICULAR EMBODIMENTS

Exemplary embodiments of the present invention will be described hereinafter, by way of example only, with reference to the accompanying drawings in which like reference signs relate to like elements and in which:

Figure 1 is a schematic overview of a system in accordance with an embodiment of the invention;

Figure 2 is a flow diagram summarising an example of the operation of the system of Figure 1;

Figure 3 is schematic overview of a client station of the system of Figure 1;

Figure 4 is a flow diagram summarising an example of the operation of the client station of Figure 3;

Figure 5 is schematic overview of a server of the system of Figure 1;

Figure 6 is a flow diagram summarising an example of the operation of the server of Figure 5;

Figure 7 is schematic overview of a communications device of the system of Figure 1;

Figure 8 is a flow diagram summarising an example of the operation of the communications device of Figure 7;

Figure 9 is schematic overview of a part of an example of a communications device of Figure 7.

DESCRIPTION OF PARTICULAR EMBODIMENTS

A particular embodiment of the present invention is described hereinafter based on the Internet and a GSM (Global System for Mobiles) mobile communication network. It should be understood that the present invention is applicable to other computer and communication networks and that the particular embodiment described herein is merely one specific implementation.

Figure 1 illustrates an overview of an embodiment of the present invention implemented using the Internet and a GSM network. An embodiment of the present invention provides secure authentication for a user access to a network resource, for example a service provided by a server on the Internet.

At a user computer 10 (for example a personal computer (PC)), a user requests access to a resource (for example for logging on to a secure website) using software at the client station (for example a Web browser). For example, the user can use a Web page relating to a resource to be accessed and enter appropriate login information

including, for example, a user identification (user-ID). In response to the user access request, the Web browser sends (12) over the Internet an access message including identification of the resource to which the user requires access and also the user-ID. The access message is received (16) from the Internet at a server 20. The server 20 can, for example, be a Web server.

The server 20 includes a directory associated with a resource that can be accessed. The directory includes user-IDs and associates a contact address (in the present example a telephone number) for a user with the appropriate user-ID. The server 20 then causes an SMS (Short Message Service) authentication request to be sent (18) over the GSM network 22. The SMS authentication request includes the user-ID and details of the resource for which an access request has been received by the server 20. The SMS authentication request is received (24) via a wireless link at communications equipment 30.

In the present instance the communications equipment is mobile equipment in the form of a mobile telephone 30 that is owned by the user and includes a proactive SIM card. By a proactive SIM card is meant a SIM card that can comprise active software for carrying out pre-programmed tasks. The communications equipment 30 is configured to alert the user of receipt of the SMS authentication request and to solicit from the user entry of a response. The user enters the response using, for example, a keyboard of the communications equipment 30 and the communications equipment is further configured to compose and send (24), via the wireless link, an SMS authentication response message. The SMS authentication response message includes the user-ID and at least a response field. The SMS authentication response message is received (28) from the GSM network 22 at the server 20.

As well as containing contact addresses associated with the user-IDs, the directory can also contain an identification of an appropriate authentication response that is to be expected in reply to the authentication request message. Accordingly, the server 20 can evaluate and verify whether the response field of the received authentication response corresponds to that expected for the user-ID in question. If a correct response is received, then access to the network service requested by the user is permitted, and an appropriate acknowledgement is sent (32) via the Internet to be received (34) by the user computer 10. If no authentication response is received by the server 20 within a predetermined time, or an authentication response as received is invalid, then an appropriate notification of this is sent 32 via the Internet 14 to be received 34 by the user's computer 10.

Figure 2 is a flow diagram illustrating the main functions performed in operation of the system of Figure 1.

In step S1, the access request is generated at the computer 10 in response to input from the user.

In step S2, the access requested generated at the user computer 10 is received by the server 20 and the server generates an authentication request message to be sent to the communications equipment 30 of the user.

At step S3, the communications equipment 30 of the user receives the authentication request, solicits a response from the user and provides a response message to be sent to the server 20.

At step S4, the server 20 receives the response message and either permits or refuses access to the resource identified in the original access request depending on whether a valid response is provided, or not.

Figure 3 is a schematic overview of components of the user computer 10. This includes a processor 40 that is connected to a display 42 for displaying, among other things, a page from a Web Browser 44. The processor 40 is also connected to storage 46, to user input devices such as a keyboard 48 and a mouse 50 and further to a

network interface 52, for example a modem, ISDN terminal adapter or the like. It will be noted that Figure 3 is schematic only, and the components of the computer 10 can be arranged in any conventional manner, for example with various functional components connected via a bus (not shown). The network interface 52 is operable to send (12) an access request message and to receive (34) a message giving notification as to whether the access request is granted, or not.

Figure 4 is a flow diagram illustrating operations performed by the user computer 10 in an example of operation of an embodiment of the invention.

At step S11, the user selects an access request. This can be achieved, in a conventional method, by selecting an icon on a web page displayed 44 by means of a Web Browser, which icon identifies that the user wishes to request access to a particular resource. In step S12, the software in the user computer 10 is operable to compose an access request message that includes a user-ID for the user concerned and an identification of the resource to be accessed. As mentioned above, the user ID can be input by the user as part of a login procedure along with, for example, a password.

In step S13, the access request message is transmitted 12 to the Internet, to be passed to the server 20.

Subsequently, following processing by the server 20, the computer 10 will receive the result of the access request at step S14 by means of an appropriate message from the server.

In step S15, the result of the access request will be displayed to the user. This can take the form of changing the display to one that includes information resulting from the requested access. Alternatively, in the event that access is refused, an appropriate display can be shown indicating the reasons why access is refused (for example, that the authentication response given by the user was invalid).

Figure 5 is a schematic overview of the server 20. As shown in Figure 5, the server 20 comprises a number of server components. Thus a World Wide Web (WWW) server 56 is operable to receive (16) the access request message from the Internet 14 and to transmit (32) an appropriate message giving notification of the result of the access request. The WWW server 56 is connected via a link 58 to an application server 60 that contains logic to drive the authentication process of the present invention. In particular, the application server 60 is responsive to receipt of an access request message via the WWW server 56 to access the directory 64 which contains information including the user-ID (UID) 61 and, associated therewith, an appropriate contact addresses (for example telephone numbers T#) 63 for the user. In addition, an indication of a valid response (VR) 65 to an authentication request message could be included, as well as other data (not represented) relating to the user.

The application server 60 is operable, in response to receipt of an access request message to compose and issue an authentication request message that is sent via a link 66 to an Over The Air (OTA) server 68 that provides an interface between the server 20 and an element of a GSM network. In the instance shown, the OTA server 68 is connected via a link 72 (for example by a digital network such as an X.25 network) to the Short Message Service (SMS) Service Centre (SMSSC) of a GSM network provider. The authentication request is sent (18) to the SMSSC 70, which in turn causes a SMS message to be sent via the GSM network 22 to the communications equipment 30 of the user at the contact address identified by the telephone number T#. By including the user-ID in an authentication request message, this information can be communicated to the communications equipment 30. The authentication message can be encrypted using any desired encryption protocol; for example an encryption protocol based on PKI or symmetric key encryption.

On subsequent receipt of a SMS message providing a response to the authentication request, the SMSSC 70 will return (28) the response via 72 to the OTA server 68 which in turn sends the response message via link 66 to the application server. By including the user-ID in the response message, the application server is able to identify the authentication request relating thereto. Moreover, the application server is configured to evaluate the response received, for example by comparing a specific response field in the response message to a valid response VR 65 as held in the directory 64 associated with the user-ID 61. If the response field of the response as received corresponds to the valid response, then access can be granted to the resource requested by the user. Otherwise, access is refused.

The application server is configured to return an appropriate result via link 58 to the WWW server 56 to be passed (32) via the Internet back to the user computer 10. The result as communicated will either be the granting of access, or an indication of why access was refused, depending on whether, or not, a valid response to the authentication response is received within a predetermined time.

The server 20 can be implemented using conventional server equipment comprising appropriate network interfaces, one or more processors and appropriate memory. The directory 64 could be configured in any appropriate manner, for example as a table, as a link list, and using any appropriate protocol, for example the Lightweight Directory Access Protocol (LDAP). Details of LDAP may be found, for example, in W Yeong, T Howes, and S. Kille, "Lightweight Directory Access Protocol", RFC 1777, March 1995.

Figure 6 is a flow diagram summarising the operation of the server 20.

In step S21, the access request message is received from the user. The access request message includes details of the resource to which the user requires access, as well as an identification of the user (UID).

In step S22, the user is identified from the UID and this is used to identify an appropriate contact address in the directory 64 for the generation of an authentication request.

In step S23, the authentication request message is sent via the GSM network as a SMS message. This includes details of the server, the access request and a request for authentication of the access request. The message can be encrypted, if required, using an appropriate protocol.

In step S24, it is assumed that an authentication response message is received.

In step S25, the authentication response is verified. The verification can include suitable decryption, if required, and checks to see that the response is from the appropriate user and is as expected. This can be achieved by comparing the received response to a valid authentication response as held in the directory 64. If the received authentication response is shown to be valid, access is permitted in step S26 to the resource and an appropriate result is sent to the user computer 10. If an invalid response is received, then access is refused at step S27 and an appropriate result is sent to the user computer 10.

Similarly, if no response is received by a given timing (time out 28), access is refused at step S27 to the resource and an appropriate result is sent back to the user computer 10.

The operation of the server 20 as described in Figure 6 can be implemented by one or more computer programs comprising computer program instructions that control the operation of one or more processors of the server 20. The computer program(s) can be held in memory of the server 20.

A computer program product comprising the computer program(s) can be supplied on a carrier medium. The carrier medium could be a storage medium, such as solid state magnetic optical, magneto-optical or other

storage medium. The carrier medium could be a transmission medium such as broadcast, telephonic, computer network, wired, wireless, electrical, electromagnetic, optical or indeed any other transmission medium.

Figure 7 is a schematic block diagram giving an overview of communications equipment 30 in the form of a mobile telephone. As shown in Figure 7, an aerial 74 is connected to a radio receiver unit 78 which in turn is connected to a processing unit 80. The processing unit 80 is also connected to the aerial 74 by a radio transmission unit 76. The processing unit and the radio receiving and transmitting unit 78 and 76 could be implemented as separate integrated circuits, or they could be implemented in a single integrated circuit. The processing unit can comprise one or more processors with associated memory and associated circuitry implemented using any appropriate technology. For example, it can be implemented as an ASIC. The processing unit 80 also has access to a chip 92 on a Subscriber Identity Module (SIM) card 90 that is used to validate and activate the communications equipment 30. Also shown in Figure 7 is a display 82, a keyboard 84, a loud speaker 86 and a microphone 87.

The SIM card is a smart card with special applications for use with a GSM network. A SIM card belongs to one person that has a contract with a GSM network provider. A SIM belongs to one telephone number in the GSM network. The owner of the communication equipment including the SIM card can accept the GSM network only if the SIM card is in the mobile phone and active. Typically, if it is active, the user will already have input a PIN (Personal Identification Number) code for the card, which is something he, or she, knows. In this manner, the user is securely identified in the GSM network. If not, then for example the SIM card can be programmed to require entry of PIN (or other user validation code) in response to receipt of an authentication request message. Access to the GSM network can be achieved everywhere that GSM network reception is possible, and not only with the network of his or her own provider. In this manner, the user has a secure smart card and a terminal in his or her hands.

Figure 8 is a flow diagram illustrating the basic steps provided in operation of the communications equipment 30.

In step S31, the authentication request message is received as a SMS message.

In step S32, the user is alerted on receipt of the authentication request message. In normal operation of a GSM telephone, the receipt of a SMS message will be identified by audio and/or visual indication. Thus, the telephone may beep and/or a visual indication may be given on the display of the telephone to show that a SMS message has been received. The authentication request is forwarded automatically to the proactive SIM card. The SIM card selects the right application on the SIM card and performs verification and/or decryption of the received message. The verification at the SIM card can include, for example, verification that the SMS message has been received from a server, the identity of which has been pre-programmed into the SIM card. The SIM card application then causes the communications equipment to prompt the user to enter a response to the authentication request. This can be, for example, the entry of a single yes or no for accepting or rejecting the authentication and/or to enter some other information in the form, for example of a personal identification number PIN.

In step S33, the SIM card can then compose a suitable response message. The response message can include the user-ID allowing the server to associate it with the authentication request and, for example, additional information such as a PIN and/or a password and/or other information from the SIM card (for example a contract number) and/or a predetermined response (e.g., simply a yes or no) entered by the user.

In step S34, a SMS response message could then be sent to the server from which the authentication request message was received, whereby the response message will pass back to the server 20.

If the SIM card is provided with a Subscriber Identity Module Toolkit Application Programming Interface (SIMAPI), the operation of the communications equipment 30 can be enhanced to provide any desired degree of automation of the messaging. Documents provided by the European Telecommunications Standards Institute (ETSI) of the SIMAPI can be found, for example, in technical specifications identified as ETSI TS 101 267, V 7.3.1 (1999-07), ETSI TS 100 977, V 7.4.0 (1999-12), ETSI TS 101 413, V 7.1.0 (1999–07) and ETSI TS 101 476, V 7.0.0 (1999–11), which documents are available from ETSI, F-06921 Sophia Antipolis, Cedex, France.

A SIM card application for implementing the program at the SIM card can be provided on the SIM card using any programming language operable under the SIMAPI. Such a program performs steps of: validating an authentication message from a server, prompting a user to input a response, preparing an authentication response message and forwarding an authentication response message to the server. In an example implementation, the SIM card application can be implemented using the Java language. Java is a trademark of Sun Microsystems, Inc.

Figure 9 is a schematic overview of the SIM Toolkit framework provided in accordance with the ETSI technical specifications mentioned above. A GSM framework 94 comprises a GSM applet and a file systems object. It provides a GSM low-level package and a SIM access package that allows applets to access GSM files. A toolkit framework 96 provides for applet triggering, command handling, and the installing and uninstalling of applets, as well as security management. The applets that may be triggered include toolkit applets 104 and application applets 106. Applets may be triggered in response to receipt of a SMS message. Thus, on receipt of a SMS message, an application applet can be provided for providing processing of authentication messages at the communications equipment 30, for example in accordance with the process steps as described with respect to Figure 8.

In summary, an embodiment of the present invention allows the user with communications equipment such as a GSM mobile telephone, which user has a contract with a communications service provider (e.g., a GSM network provider) that assigns a unique address (e.g., telephone number) to the communications equipment. A server is provided with this communications address and links it to a user-ID that is, for example, assigned by the server to the user. The communications equipment thus provides a mechanism for receipt of and response to an authentication message from the server.

For example, where the user requests a secure website with his or her user-ID, the server will send an authentication message (e.g., a SMS message) to the communications address, e.g. a telephone number, associated with the user-ID. The communications equipment will receive the authentication request, will request the user to accept the authentication request and to return an appropriate response message to the server with confirmation that the user accepts the authentication request message. The server will receive the response message and complete the login of the user to the secure website, or not, dependent on whether a valid response from the user is received. By including the user-ID, and possibly also an identification of the resource to be accessed in each message sent, related messages can easily be linked to one another. Alternatively, another message format could be used with another mechanism (for example a serial number) for identifying related messages.

An embodiment of the invention can be implemented by providing the server with a database that links user-IDs to the communications addresses for the user. Readily available communications equipment can be used

at the user side. If required, additional information (for example geographic information) can be submitted with the response from the communications equipment to the server. The process can be enhanced through the use of cryptographic keys (for example with symmetric keys using a challenge response, or with public keys using certificates).

Although a particular embodiment of the invention has been described, it will be appreciated that many modifications, additions and substitutions may be made within the spirit and scope of the invention.

Thus, for example, although the invention has been described in the context of the Internet and a GSM network, the invention is not limited thereto and could be implemented over any other network and using any other form of additional network for communication with the user. For example, networks using standards other that GSM are known or planned. Networks that are currently planned for the future include the use of a validation device that confirms the contract between the user and a service provider. The user can only then get access to the network where a valid validation device is present in the equipment. It will be appreciated that the invention can be applied in such systems, even where the validation device is not a SIM. More generally, communication with the user could be via another form of wireless communication network, or by satellites, networks, landlines or indeed any other form of telecommunications network.

An embodiment of the invention can also be envisioned that is operable whether or not a validation device such as a SIM card is provided in the communications equipment. Thus, for example, a message (for example a text message such as a SMS message), or an automated voice message, could be sent to the user on his or her communications equipment. This message could solicit a response from the user to authenticate a resource access request. The entry of a text or voice response could then be analysed by the server, using text comparison or voice recognition technology, to verify that the response corresponds to a predetermined response pre-recorded at the server. If the response checks out, then access to the resource can be permitted.

Although an implementation of the invention has been described in the context of a mobile telephone forming the user communications equipment, it will be appreciated that other forms of user communications equipment can be employed. Thus, for example, the communications equipment could be by means of a WAP (Web Access Protocol) telephone, by a personal assistant with a communications interface, or indeed by any other form of communications equipment that can be addressed directly by the server to solicit a response to an authentication message. The use of a different channel for communication with the user than that used for the direct web access to verify the access request enhances security of access.

Also, although a manual input is provided by the user, by linking the communications device to the station that originated the access request (for example by means of a WAP phone), the whole process can be automated, whereby information is passed between the web browser at which access is requested, and a further application provided for responding to the authentication request.

WHAT IS CLAIMED IS:

1. Network access security system comprising:
a client station for inputting an access request for access to a resource via a network, the access request identifying the user and the resource to be accessed;
a server holding data relating to users including a contact address for a communications device for users, the server being responsive to a received access request to issue an authentication request to the communications device of a user identified in the access request, and
a said communications device including a receiver for receiving the authentication request from the server, a controller operable to invite a response to the authentication request and a transmitter to return the response to the server;
wherein the server is further operable to evaluate a received response for determining whether the user is permitted to gain access to the resource.

2. The system of claim 1, wherein at least one of the receiver and the transmitter includes a wireless communications interface.

3. The system of claim 2, wherein the communications device is a mobile telephone.

4. The system of claim 1, wherein the communications device includes a user identification unit.

5. The system of claim 4, wherein the user identification unit is a SIM card.

6. The system of claim 5, wherein the communications device is a GSM telephone.

7. The system of claim 1, wherein the authentication request messages is a text message.

8. The system of claim 1, wherein the response message is a text message.

9. The system of claim 1, wherein at least one of the authentication message and the response message is a Short Message Service message.

10. The system of claim 1, wherein the network is the Internet.

11. A communications device including a receiver for receiving a resource access authentication request from a server, a controller operable to invite a response to the authentication request, and a transmitter to return the response to the server.

12. The device of claim 11, wherein the receiver comprises a wireless signal receiver.

13. The device of claim 11, wherein the transmitter comprises a wireless signal transmitter.

14. The system of claim 11, wherein the communications device is a mobile telephone.

15. The system of claim 11, wherein the communications device includes a user identification unit.

16. The system of claim 15, wherein the user identification unit is a SIM card.

17. The system of claim 16, wherein the communications device is a GSM telephone.

18. The system of claim 11, wherein the authentication request messages is a text message.

19. The system of claim 11, wherein the response message is a text message.

20. The system of claim 11, wherein at least one of the authentication message and the response message is a Short Message Service message.

21. A server including a network message interface for receiving an access request from a client station for access to a resource, the access request identifying the user, a server holding data relating to users including at least a contact address for a communications device for users, the server being responsive to a received access request to issue an authentication request to the communications device of a user identified in the access request.

22. The server of claim 21, comprising a directory holding the data relating to users, and a controller responsive to receipt of an access request to retrieve a contact address from the directory for the user and to issue an authentication request to the communications device.

23. The server of claim 21, wherein the authentication request is directed via a message service for calling the communications device of the user.

24. The server of claim 21, wherein the directory holds required responses to authentication requests, the controller being operable to evaluate a response received from the communications device to determine whether to permit access to the resource.

25. The server of claim 21, wherein the network is the Internet.

26. A network client comprising user input equipment for input of a resource access request, a mechanism for composing an access request identifying the user and the resource to be accessed, and a network interface for issuing an access request to a server for access to a network.

27. A method of controlling access to a network resource, comprising:
in response to the input of an access request by a user for access to a resource at a network client, issuing an access request to a server, the access request identifying the user and the resource to be accessed;
at the server, responding to receipt of the access request to retrieve a contact address for a communications device for the user identified in the access request to issue an authentication request to the communications device;
at the communications device, responding to receipt of the authentication request to invite a response to the authentication request and transmitting the response to the server; and
at the server, evaluating the response and, in the event of a valid response, permitting access to the resource.

28. The method of claim 27, communications device is a device for wireless communication.

29. The method of claim 28, wherein the communications device is a mobile telephone.

30. The method of claim 29, comprising, at the communications device, extracting user information from a user identification unit.

31. The method of claim 30, wherein the user identification unit is a SIM card.

32. The method of claim 31, wherein mobile telephone is a GSM telephone.

33. The method of claim 27, wherein the authentication request messages is a text message.

34. The method of claim 27, wherein the response message is a text message input by a user via the mobile telephone.

35. The method of claim 27, wherein at least one of the authentication message and the response message is a Short Message Service message.

36. The method of claim 27, wherein the network is the Internet.

37. A computer program product on a carrier medium, the computer program product comprising program instructions for controlling a server:
to determine a contact address for a communications device of a user associated with a user identification in a resource access request received from a client station;
to issue an authentication request to the communications device at the retrieved address;
to evaluate a response received from the communications device and to permit access to the requested resource only where a valid response is received.

38. A computer program product on a carrier medium for controlling a proactive validation unit in mobile equipment, the computer program comprising program instructions to validate an authentication message received from a server, to prompt a user to input a response, to prepare an authentication response message and to forward an authentication response message to the server.

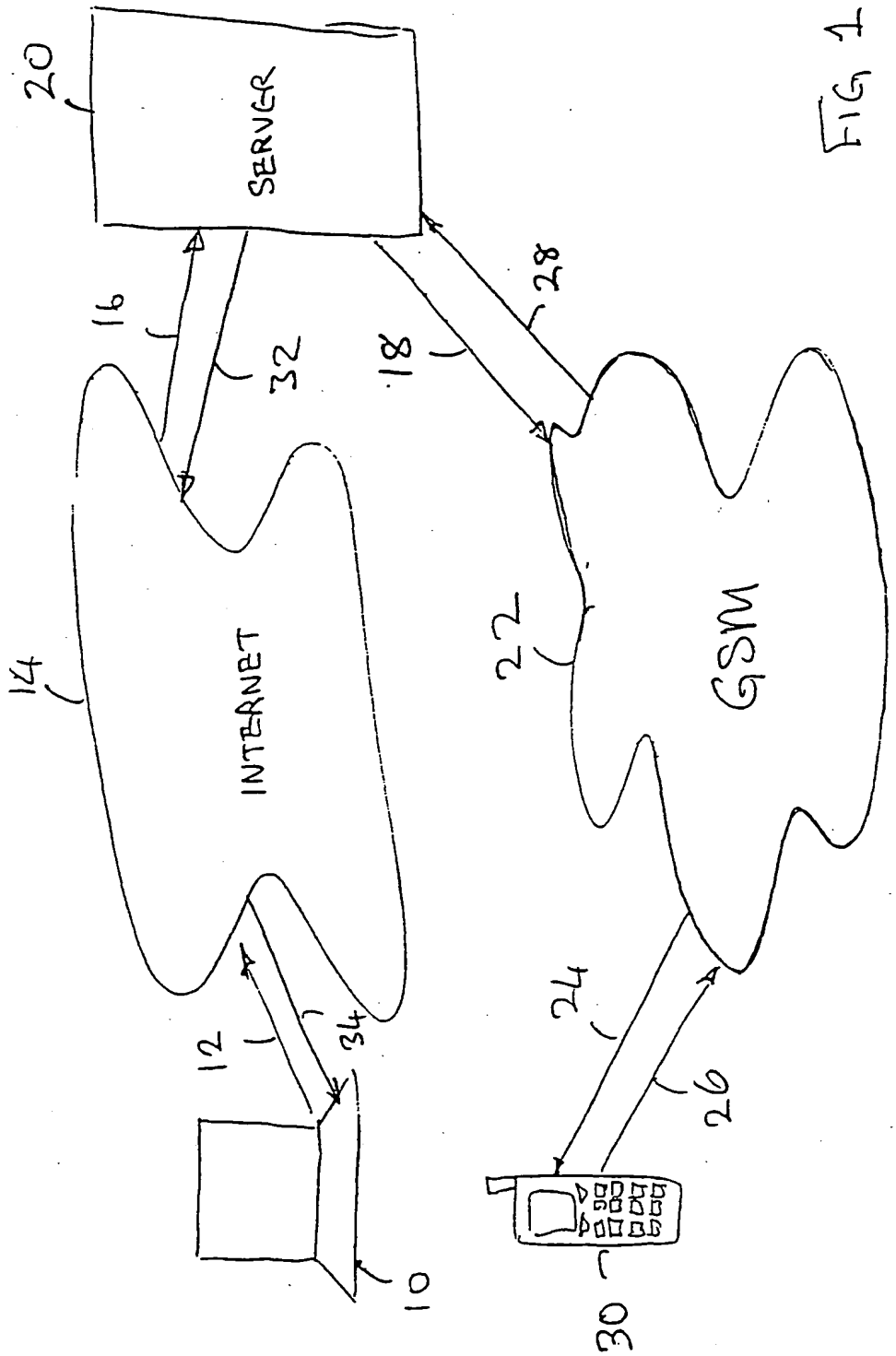


FIG 1

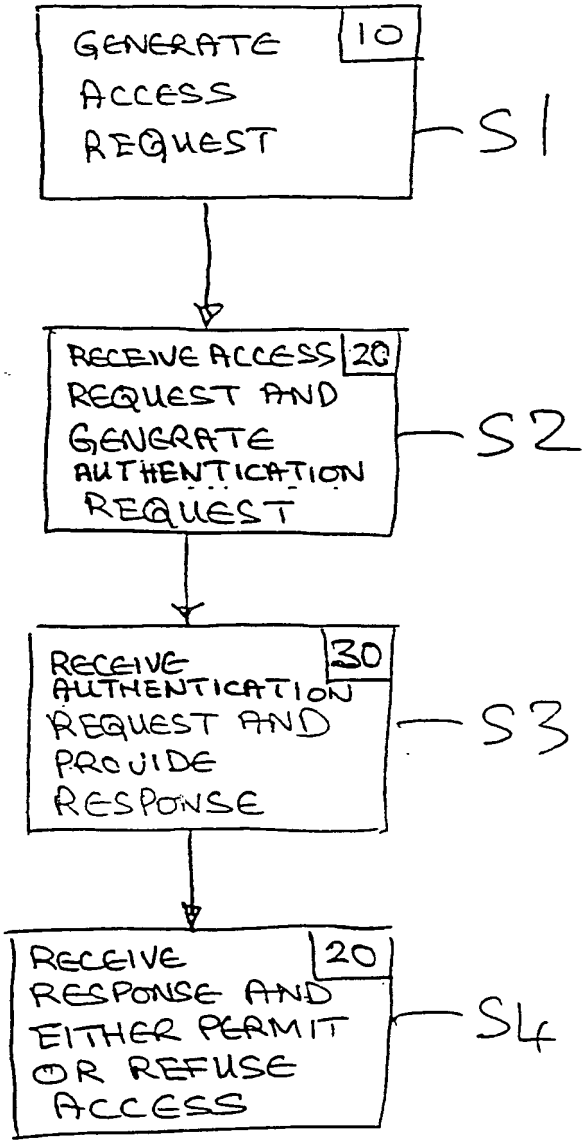

GENERATE ACCESS REQUEST
10
S1
RECEIVE ACCESS REQUEST AND GENERATE AUTHENTICATION REQUEST
20
S2
RECEIVE AUTHENTICATION REQUEST AND PROVIDE RESPONSE
30
S3
RECEIVE RESPONSE AND EITHER PERMIT OR REFUSE ACCESS
20
S4

FIG 2

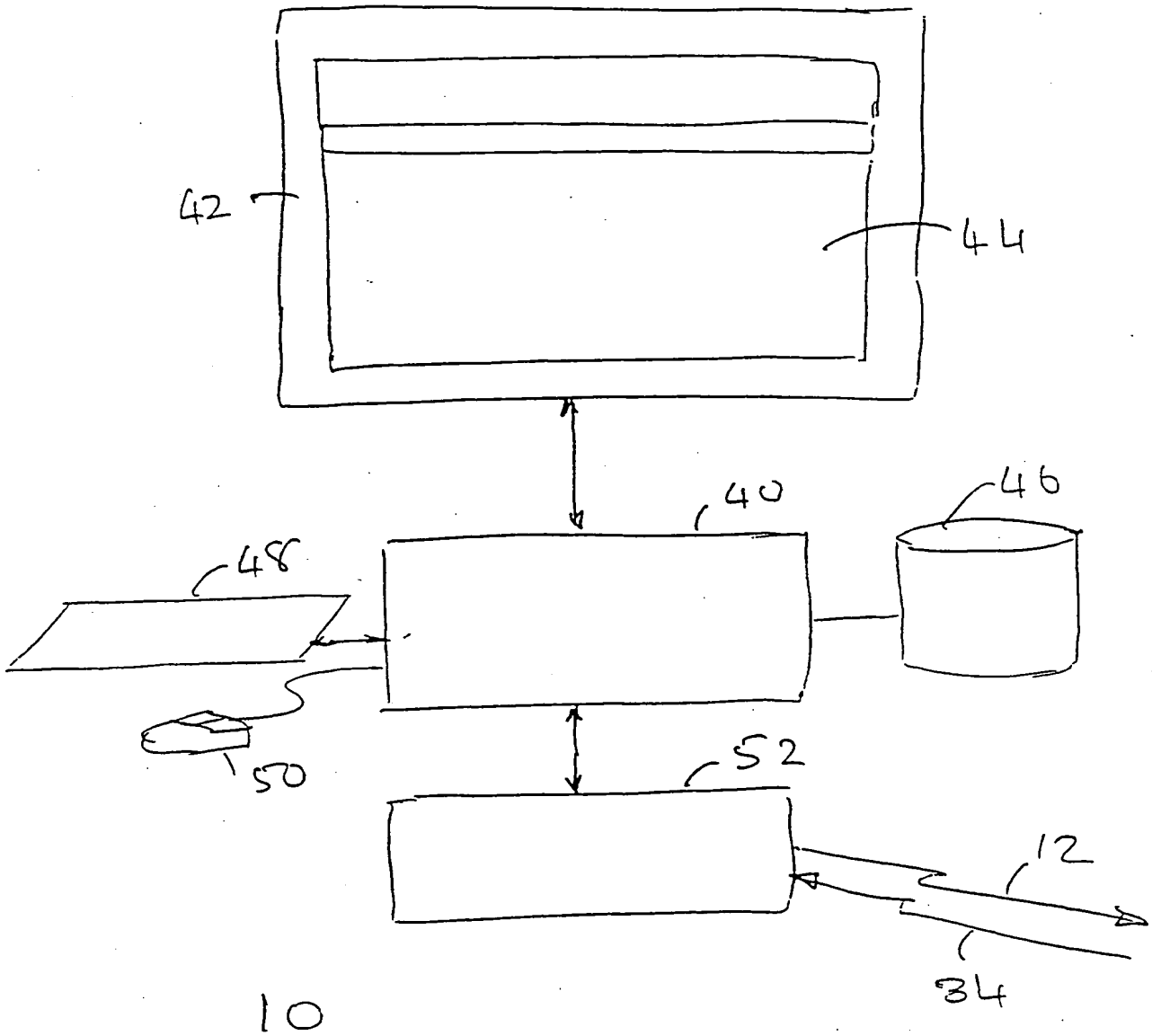


FIG. 3

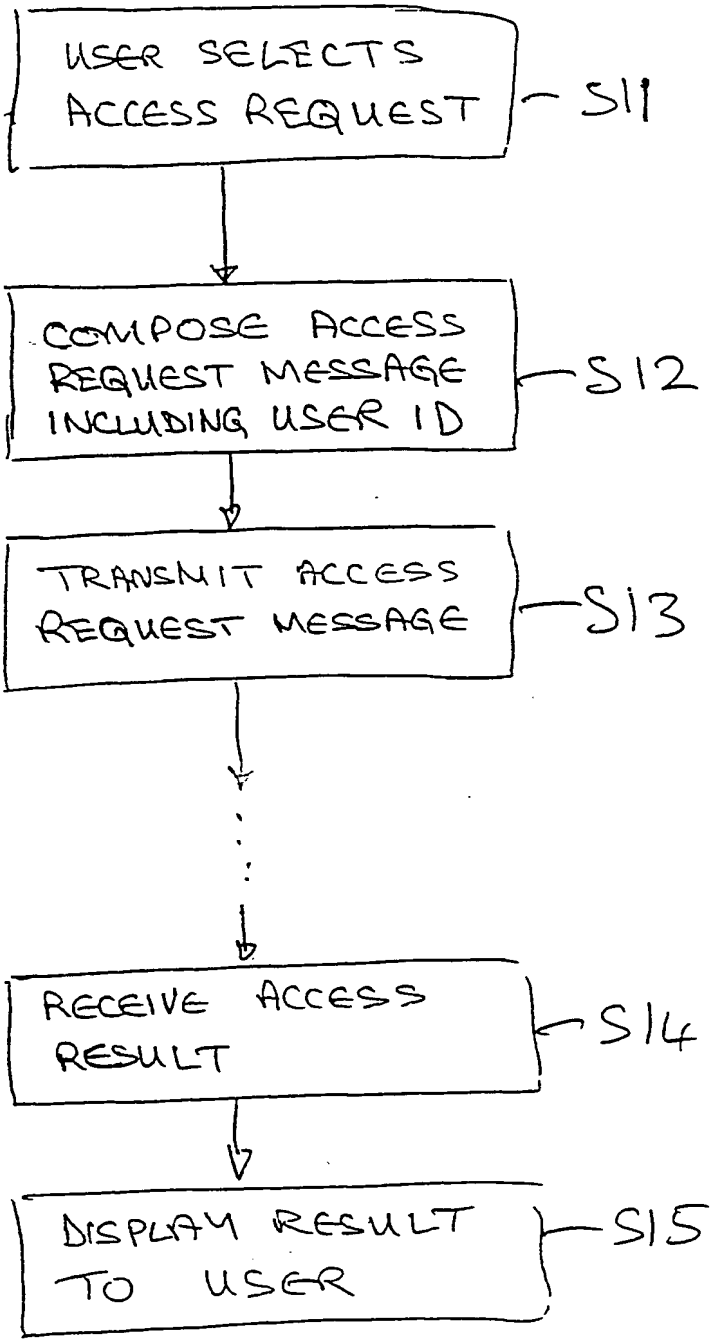

USER SELECTS ACCESS REQUEST
S11
COMPOSE ACCESS REQUEST MESSAGE INCLUDING USER ID
S12
TRANSMIT ACCESS REQUEST MESSAGE
S13
RECEIVE ACCESS RESULT
S14
DISPLAY RESULT TO USER
S15

FIG 4

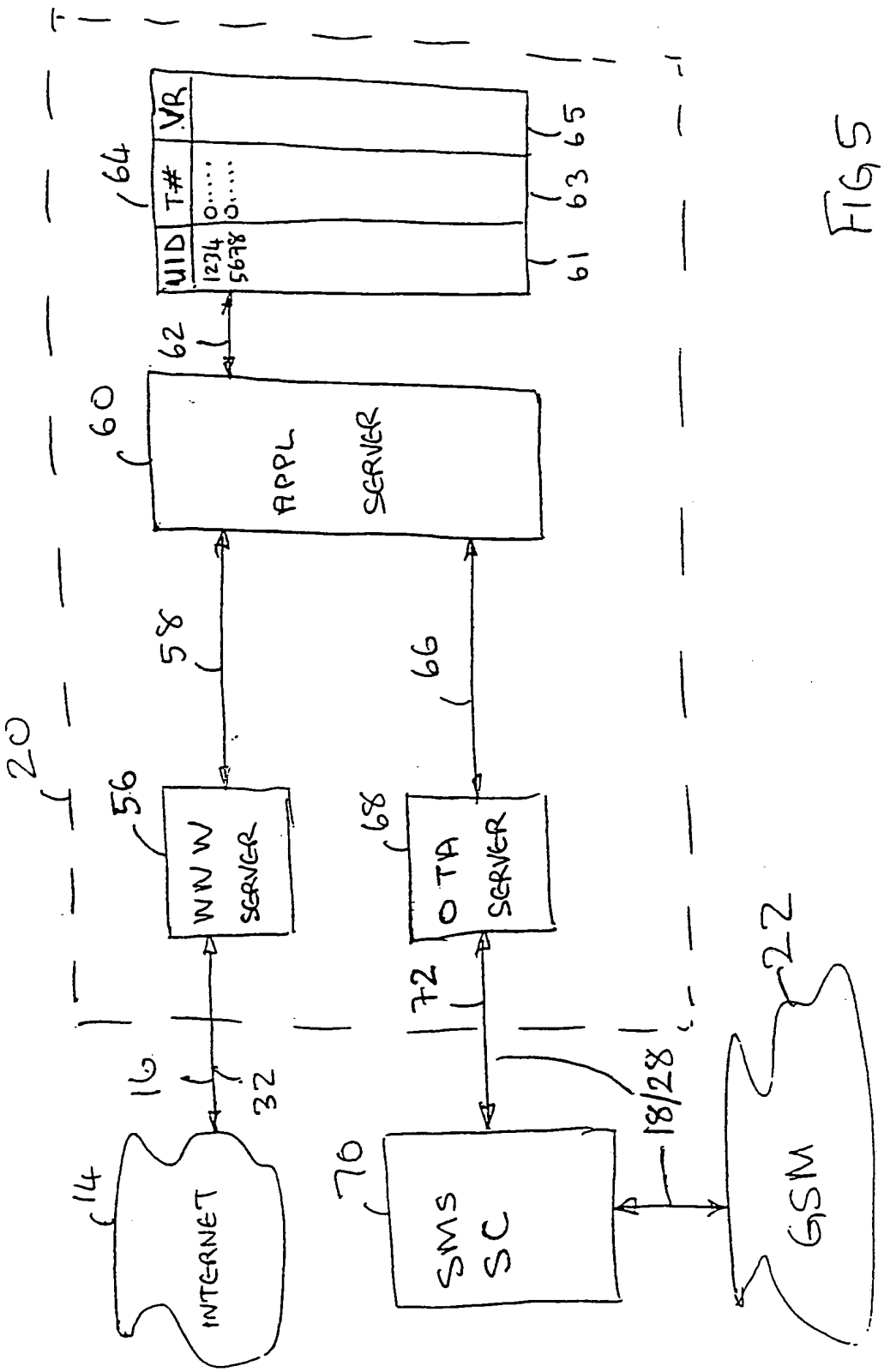

UID
T#
VR
1234
5678
64
65
63
61
62
60
APPL SERVER
58
66
20
56
WWW SERVER
68
OTA SERVER
16
32
72
18/28
14
INTERNET
70
SMS SC
22
GSM

FIG 5

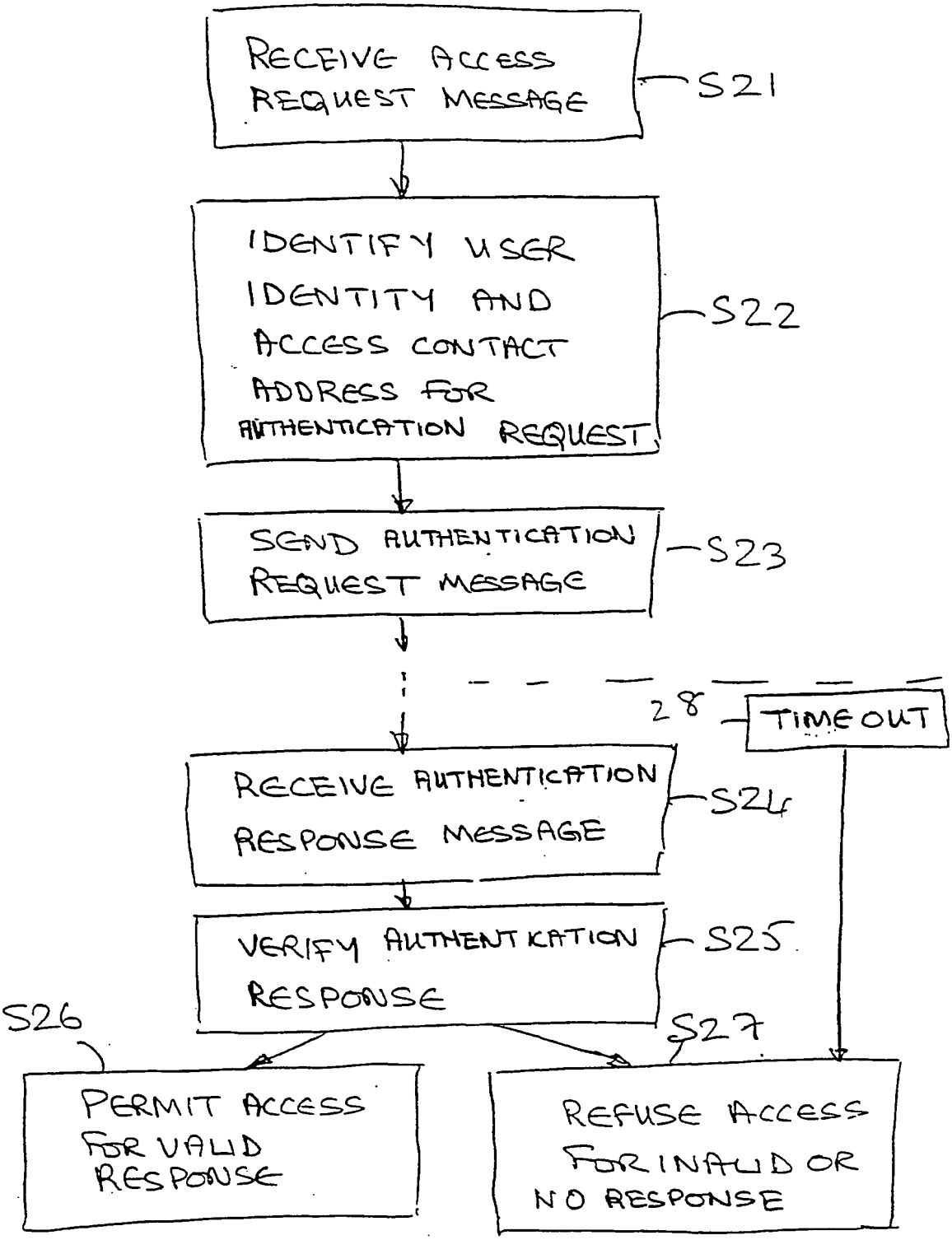

RECEIVE ACCESS REQUEST MESSAGE
S21
IDENTIFY USER IDENTITY AND ACCESS CONTACT ADDRESS FOR AUTHENTICATION REQUEST
S22
SEND AUTHENTICATION REQUEST MESSAGE
S23
28
TIMEOUT
RECEIVE AUTHENTICATION RESPONSE MESSAGE
S24
VERIFY AUTHENTICATION RESPONSE
S25
S26
S27
PERMIT ACCESS FOR VALID RESPONSE
REFUSE ACCESS FOR INALID OR NO RESPONSE

FIG 6

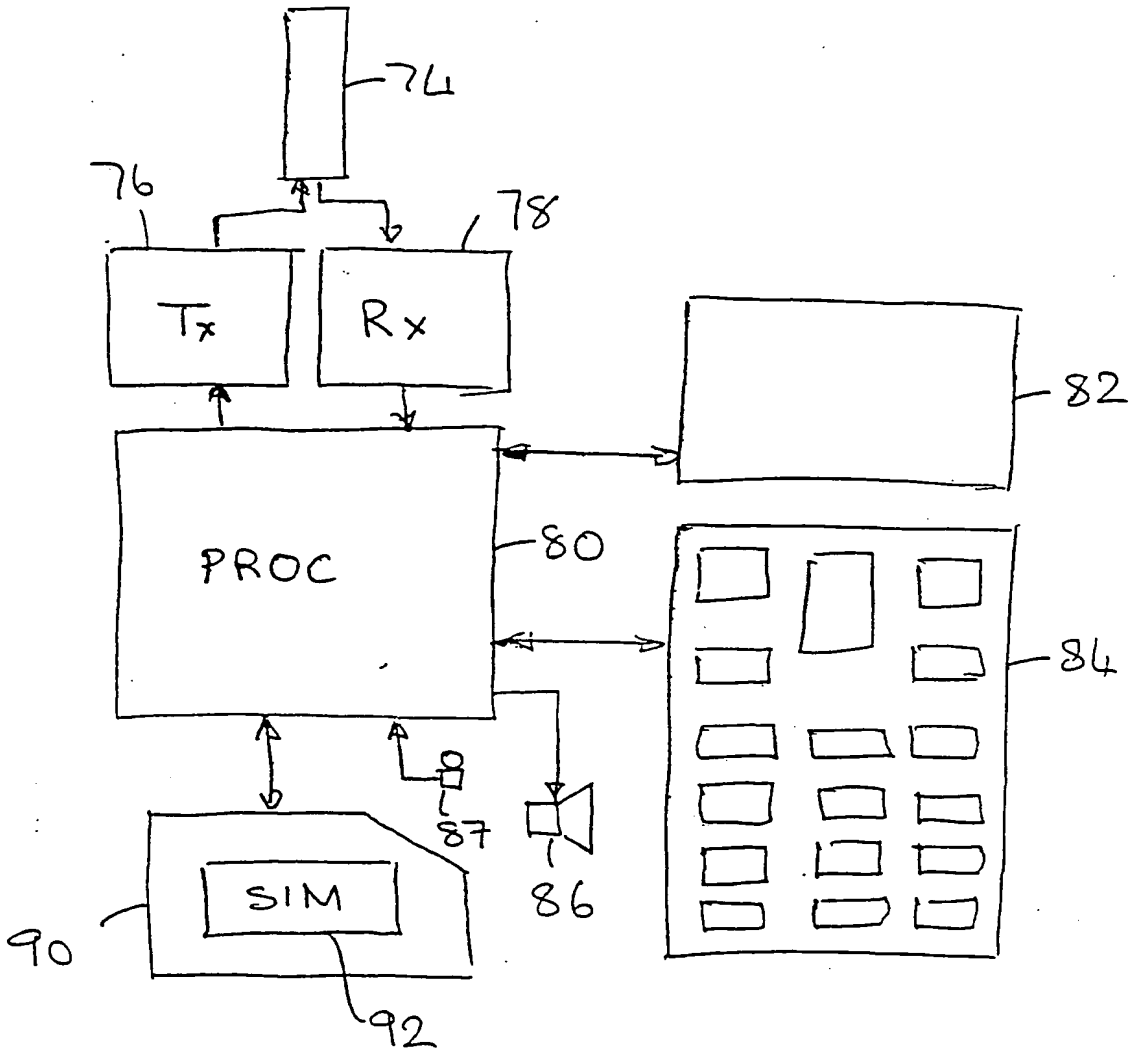


FIG 7

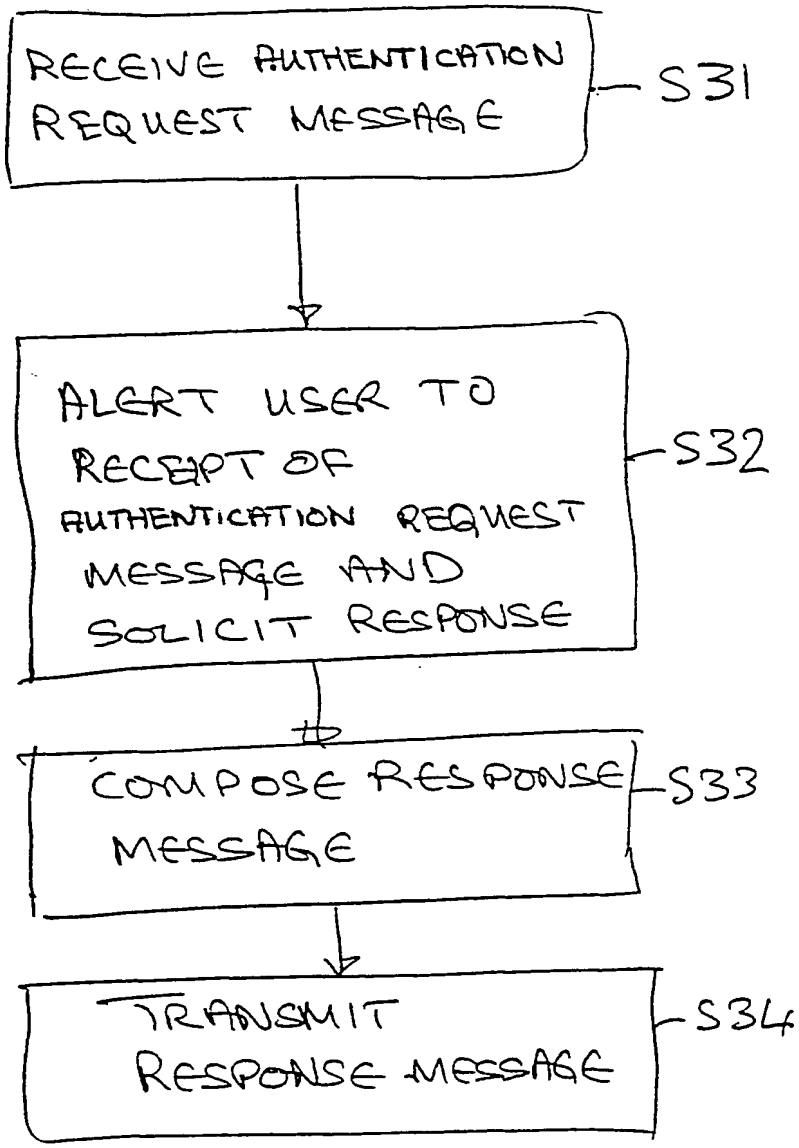

RECEIVE AUTHENTICATION REQUEST MESSAGE
S31
ALERT USER TO RECEIPT OF AUTHENTICATION REQUEST MESSAGE AND SOLICIT RESPONSE
S32
COMPOSE RESPONSE MESSAGE
S33
TRANSMIT RESPONSE MESSAGE
S34

FIG 8

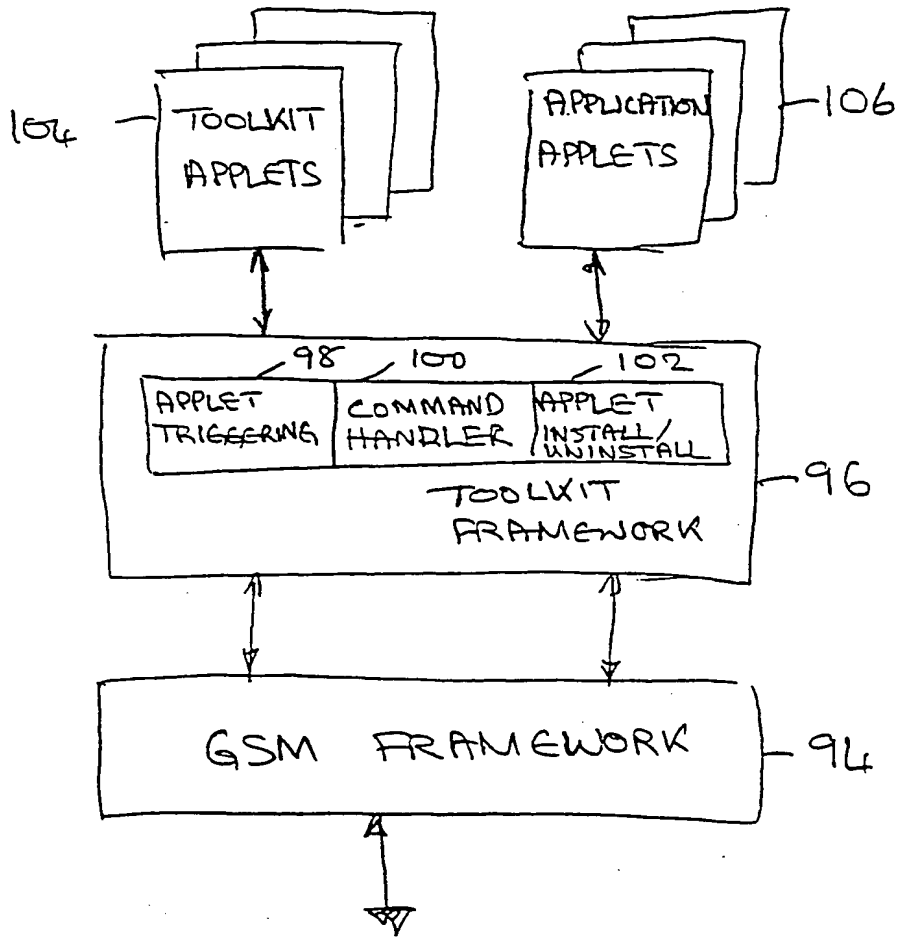

104
TOOLKIT APPLETS
APPLICATION APPLETS
106
98
100
102
APPLET TRIGGERING
COMMAND HANDLER
APPLET INSTALL/ UNINSTALL
TOOLKIT FRAMEWORK
96
GSM FRAMEWORK
94

FIG 9

INTERNATIONAL SEARCH REPORT

Int ional Application No
PCT/US 01/05261

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, PAJ, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	NL 1 007 409 C (KONINKLIJKE PTT NEDERLAND N:V:) 18 November 1997 (1997-11-18) the whole document	1-21, 23-38
X	WO 95 19593 A (KEW MICHAEL JEREMY ;LOVE JAMES SIMON (GB)) 20 July 1995 (1995-07-20) page 1, line 20 -page 2, line 36 page 7, line 10 -page 9, line 11	1-3,6, 11-14, 17,21, 22,24, 26-29, 32,37,38

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
21 September 2001	08/10/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Brichau, G

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 01/05261

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P,X	FR 2 795 264 A (LENOIR OLIVIER) 22 December 2000 (2000-12-22) page 1, line 13 -page 6, line 6	1-6, 10-17, 21,22, 24-32, 36-38

Form: PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Int[illegible]onal Application No
PCT/US 01/05261

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
NL 1007409 C	18-11-1997	NL 1007409 C1	18-11-1997
WO 9519593 A	20-07-1995	AU 1390395 A	01-08-1995
		WO 9519593 A1	20-07-1995
		GB 2300288 A	30-10-1996
FR 2795264 A	22-12-2000	FR 2795264 A1	22-12-2000
		AU 6287300 A	02-01-2001
		WO 0078009 A2	21-12-2000